

# Fact Sheet

## **National Cybersecurity & Communications Integration Center (NCCIC)**

### **Background**

The communications sector and the information technology (IT) sector are both essential to national and economic security, public health and safety, and the provision of vital government services. Their functions are especially critical during emergencies. The ability to quickly and reliably communicate in times of crisis can make the difference between life and death, success or failure.

The government and industry treat these sectors as separate and distinct, with their own organizational structures under the National Infrastructure Protection Plan (NIPP) framework. However, technological advances continue to blur the distinction between them. The convergence of traditional voice and more modern data networks have created an increasingly seamless system for transmitting information. Increasingly, next generation networks are able to convey both data and communication over the same system. Therefore, technological convergence of the information technology (IT) and communications sectors requires that we update and integrate incident response mechanisms used to mitigate malicious activity that could potentially disrupt critical functions and services provided by these sectors.

### **National Cybersecurity & Communications Integration Center (NCCIC)**

On October 30, 2009, the Department of Homeland Security (DHS) activated the National Cybersecurity & Communications Integration Center (NCCIC). The establishment of NCCIC was led by DHS and is the culmination of work resulting, in part, from a series of recommendations by a Joint *Industry-Government Tiger Team*, the National Security Telecommunications Advisory Committee (NSTAC) and the Government Accountability Office. These recommendations emphasized the need for collocation, integration, and eventual interoperability of existing cyber and communications incident response mechanisms into a unified operations center.

NCCIC will improve the nation's capability and capacity to detect, prevent, respond, and mitigate disruptions of voice and cyber communications risks. NCCIC unifies vital IT and Communications operations centers thereby converging existing incident response mechanisms and better reflecting the reality of technological convergence.

The new unified operations center combines two of DHS's operational organizations: National Coordinating Center for Telecommunications (NCC) and United States Computer Emergency Readiness Team (US-CERT). The NCC is the operational arm of the National Communications System. It provides a mechanism to coordinate initiation and restoration of national security/emergency preparedness (NS/EP) telecommunications services at times of crisis. It is a joint industry and government-staffed center to handle emergency telecommunications requests. During emergencies it assesses damage, identifies NS/EP requirements and prioritizes restoration efforts. The NCC is a 24/7/365 operations watch center.

US-CERT, created in 2003 by DHS, is the operational arm of the National Cyber Security Division. It is identified by OMB, under FISMA, to serve as the Federal information security incident center. US-CERT's mission includes: analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems. Operating a 24/7/365 operations center, US-CERT is the lead entity in the national effort to provide timely and effective technical assistance to operators of agency information systems regarding security incidents. This includes providing guidance on detecting and handling information security incidents; compiling and analyzing information about incidents that threaten information security; and informing operators of agency information systems about current and potential information security threats and vulnerabilities. Additionally, US-CERT provides consolidated intrusion detection, incident analysis, and cyber response capabilities to secure federal agencies' external access points, including access to the Internet, for all Federal Executive Branch networks and systems.

### **Phase One**

The NCCIC brings together the most successful elements of its predecessors while adding greater efficiency, transparency, integration, and collaboration. DHS is taking a phased approach as it builds the NCCIC. The first phase of operations is the integration of the government components – NCC and US-CERT. In addition, elements of DHS's Office of Intelligence and Analysis (I&A) and the National Cyber Security Center (NCSC) will be functionally integrated into the new center. Over time, all of these elements will be collocated in the new facility. Each organization will share information as authorized, build relationships and work jointly when situations demand.

### **Phase Two**

The second phase of the NCCIC will include DHS's private sector partners. Private-public partnerships are critical to protect the nation's IT and communication infrastructure. The NCC, the telecommunications operations center, already has a number of on-site private industry representatives from the communications sector. These representatives will be incorporated gradually and will maintain a similar working model until new standard operating procedures for handling steady state and crisis operations are created and adopted by both industry and government. This includes industry representatives located on the watch floor who will interact with government counterparts to share relevant information. These actions and activities will facilitate timely and effective crisis operations in the event of a significant service disruption or cyber incident.